IN THE UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF PENNSYLVANIA

IN RE PROSPECT MEDICAL HOLDINGS, INC. DATA BREACH LITIGATION	Case No: 2:23-CV-03216 ORAL ARGUMENT REQUESTED

REPLY IN SUPPORT OF DEFENDANT'S MOTION TO DISMISS

DUANE MORRIS LLP
Alan C. Kessler
Luke P. McLoughlin
Ryan Monahan
Lauren Pugh
30 S. 17th Street
Philadelphia, PA 19103
LPMcLoughlin@duanemorris.com

-and-

Gerald L. Maatman Jr.
Jennifer A. Riley
DUANE MORRIS LLP
190 South LaSalle Street, Suite 3700
Chicago, IL 60603-3433

Counsel for Prospect Medical Holdings, Inc.

Prospect Medical Holdings Inc. ("Prospect"), by and through its undersigned counsel, respectfully submits this Reply in further support of its Motion to Dismiss.

SUMMARY OF ARGUMENT

Plaintiffs' Complaint arises out of a third-party attack on Prospect's systems and a resulting data breach. Prospect moves to dismiss because (1) Plaintiffs' threadbare allegations of hypothetical harm arising from the data breach do not confer Article III standing, and (2) even if Plaintiffs have standing, they fail to state a claim for which relief can be granted.

As to standing, Plaintiffs' response cannot obscure the simple fact that the mere existence of a data breach does not confer Article III standing. Plaintiffs point to two distinct and distant events: (1) a scattering of claimed everyday issues *e.g.*, "changing passwords" and "reviewing financial statements," Opp. at 1-2, as purported "injuries-in-fact," and (2) a standard, precautionary Notice Letter. In between those two distant poles, Plaintiffs attempt to place Prospect—and solely Prospect, despite the thousands of other entities that have the same information—at fault for Plaintiffs' non-cognizable, everyday issues, and do so solely on the basis of the very Notice that Prospect provided to them. This is the textbook threadbare allegation that is insufficient under the Federal Rules and Supreme Court precedent to advance past the pleadings stage. On these types of pleadings, courts should and do dismiss the claims.

As to the factual pleadings, Plaintiffs fail to state a claim. Plaintiffs have conspicuously retreated in the face of Prospect's detailed motion by (1) dropping and declining to defend their California Customer Records Act Claim (Count VI), and (2) dropping and declining to defend their California Medical Information Act claim filed under Section 56.10 (Count V). In a misplaced effort to shore up what remains of the Consolidated Complaint, Plaintiffs veer into *ad hominem*, making the preposterous contention that Prospect "intentionally" sought to weaken its

own health care information technology and in so doing suffer millions of dollars of business losses. Opp at. 27. Wild charges of this sort cannot rehabilitate the Consolidated Complaint. The Court should dismiss what remains of the Consolidated Complaint.

I. Plaintiffs Lack Standing

A. Plaintiffs Misapprehend the Third Circuit's Decision in *Clemens*.[1]

Prospect demonstrated that Plaintiffs lack standing under Supreme Court and Third Circuit precedent, including *Clemens v. ExecuPharm Inc*., 48 F.4th 146 (3d Cir. 2022). In response, Plaintiffs misunderstand *Clemens* and the legal requirements for standing.

Even in the data breach context, the alleged injury must be "actual or imminent" ***and*** "concrete." *Id. at* 152. A plaintiff claiming a substantial risk of identity theft or fraud must allege, not only a substantial risk of future harm, but that "the exposure to that substantial risk caused additional, currently felt concrete harms." *Id*. at 152–56. Plaintiffs concede that they principally bring claims for "future harms," Opp. at 5, but fail to adduce facts showing that such future harms are both "imminent" and "concrete."

Plaintiffs, for example, do not adduce any facts showing they suffered emotional distress, and concede that Prospect is already responsible for credit monitoring costs. Compl. ¶¶ 9, 73. *See Clemens*, 48 F.4th at 156 (recognizing as concrete "experience[ing] emotional distress or spend[ing] money on mitigation measures like credit monitoring services."). Plaintiffs instead argue that they satisfy the standing requirements by alleging that their sensitive information "was exposed and compromised as a result of a targeted attack by a ransomware gang, Rhysida." Opp. at 5. Plaintiffs claim that this allegation "alone establishes standing," because the court in

[1] Prospect addressed many of Plaintiffs' arguments in its Motion to Dismiss and Supporting Memorandum of Law ("Motion"). Prospect thus responds to the "issues newly raised in the opposing party's response." Judge Beetlestone's Practices & Procedures, Civil Cases § IV(A).

Clemens "found dispositive the fact that the plaintiff's complaint alleged that the PII was stolen by a ransomware gang." (*Id.* at 5, 7.) But Plaintiffs misapprehend *Clemens*.

The Third Circuit explained that there are "a number of factors" upon which a court can use to determine whether an injury is imminent, "*with no single factor being dispositive to our inquiry*." *Clemens*, 48 F.4th at 153 (emphasis added). The *Clemens* court directed the consideration of several factors to determine "whether an injury is present versus future, and imminent versus hypothetical" and emphasized that "a possible future injury—even one with an objectively reasonable likelihood of occurring—is not sufficient" for standing. *Id.* (citing *Clapper v. Amnesty Int'l USA*, 568 U.S. 398, 414 n.5 (2013)) (internal quotation marks omitted). Plaintiffs' possible future injury is not a basis for standing.

Plaintiffs have also not alleged what if any information *actually* was accessed. As set forth in the Notice Letter, Prospect advised individuals that information *may* have been subject to unauthorized access, which *may* have included names and Social Security Numbers. The Notice Letter's precautionary language cannot create standing, nor can Plaintiffs' allegations as to the third party ransomware gang. Those allegations are facially theoretical, relying on online chatter by an internet gang that "claims responsibility" for the attack, "indicated" that information may have been sold, and "claims to have leaked" files on the Dark Web. Compl. ¶¶ 60–62. Aside from the bizarre attempt to rely on a ransomware gang as a credible source, *Clemens* is distinct from the instant case, as it included allegations that the data was *actually* published on the Dark Web, and cited credible information confirming that the data was *actually* sensitive, and *actually* accessible by "nefarious" third parties. 48 F.4th at 157. Such allegations are not present here.

Plaintiffs' allegations more closely resemble those from *Reilly v. Ceridian Corp.*, 664 F.3d 38 (3d Cir. 2011), in which the Third Circuit held that the plaintiffs' risk of harm was

"dependent on entirely speculative, future actions" of a hacker. 664 F.3d at 42-43. The same is true here. Based on the abstract "facts" pleaded in the Complaint, a "court is still left to speculate, as in *Reilly*, whether the hackers acquired Plaintiffs' PHI in a form that would allow them to make unauthorized transactions in their names, as well as whether Plaintiffs are also intended targets of the hackers' future criminal acts." *Graham v. Universal Health Serv., Inc.*, 539 F. Supp. 3d 481, 487 (E.D. Pa. 2021).

Plaintiffs, at most, plead that the third party hackers obtained their information through a ransomware attack against Prospect, which is not sufficient to confer standing. *See id.*; *see also In re Retreat Behav. Health LLC*, 2024 WL 1016368, at *3 (E.D. Pa. Mar. 7, 2024) ("The forensic investigation performed by Defendants merely revealed that an unauthorized person may have accessed a data set including Plaintiff's personal information."). Such factually empty claims of concededly "future harms," Opp. at 5, fail to show standing. Nor do Plaintiffs' claims of lost time constitute "concrete" harm sufficient to confer standing. Opp. at 9. Updating a password or reviewing a bank statement is an ordinary part of everyday life—it is not time that is "lost," and such "mitigation costs" only constitute concrete harms if Plaintiffs have plausibly alleged a "substantial risk of identity theft." *See In re Retreat Behav. Health LLC*, at *3. (citing *Clemens*, 48 F.4th at 155-56). They have not done so here.

B. Plaintiffs Fail to Show Traceability or Injury

Even if Plaintiffs allege an injury-in-fact (and they do not), they must connect it to Prospect. Plaintiffs, at most, point to a few commonplace occurrences (e.g., spam emails, phone calls, credit card and account notifications (Opp. at 18)) and contend that those occurrences must be traceable to the Data Breach. But Plaintiffs plead no facts showing that the incidents are traceable to any action taken by Prospect. Instead, Plaintiffs try to reverse engineer traceability from the Notice Letter itself, which is not evidence of traceability. Plaintiffs nowhere allege that

their information was otherwise kept secure. Nor do they allege that they have not received other notice letters about the same information from other companies who may have experienced data breaches. These omissions are fatal. Because traceability requires more than Plaintiffs' "speculative chain of possibilities," *Clapper*, 568 U.S. at 414, this Court should dismiss the Complaint.

C. Regulatory Claims Do Not Independently Confer Standing

The Supreme Court made clear in *TransUnion* that Congress "may not . . . us[e] its lawmaking power to transform something that is not remotely harmful into something that is." *TransUnion*, 141 S. Ct. at 2205. Plaintiffs nonetheless contend that a statute can confer standing and thus a federal court's jurisdiction over a suit. Opp. at 11. Plaintiffs are mistaken. Plaintiffs cite *In re Horizon Healthcare Servs. Data Breach Litig.*, 846 F.3d 625 (3d Cir. 2017), but that case did not hold that a statute confers standing. Instead, it anticipated *TransUnion* and determined that the statutory claim did not and could not confer standing on its own. Thus, as the Third Circuit later explained: "In *TransUnion*, the cognizable harm from wrongly identifying the class members as potential terrorists was akin to the harm from defamation. In *Horizon*, the cognizable harm from the unauthorized release of the plaintiffs' sensitive information was akin to the harm from invasion of privacy." *Huber v. Simon's Agency, Inc.*, 84 F.4th 132, 153 (3d Cir. 2023). The Supreme Court has expressly "rejected the proposition that 'a plaintiff automatically satisfies the injury-in-fact requirement whenever a statute grants a person a statutory right and purports to authorize that person to sue to vindicate that right.'" *TransUnion*, 141 S. Ct. at 2205 (quoting *Spokeo, Inc. v. Robins*, 578 U.S. 330, 341 (2016)). Congress's creation of a remedy does not make harm "concrete" absent "any physical, monetary, or cognizable intangible harm traditionally recognized" in common law. *Id.* at 2206. Plaintiffs fail to establish an independent, concrete harm by referencing a statute.

II. Plaintiffs Fail to State a Claim for Relief

A. Plaintiffs Fail to State a Claim for Negligence or Negligence Per Se

Plaintiffs do not plausibly allege traceability and damages—requirements of any negligence claim. Plaintiffs point to their claim that each "suffered lost time, annoyance, interference, and inconvenience as a result of the Data Breach and has anxiety and increased concerns for the loss of [their] privacy" and "suffered imminent and impending injury arising from the substantially increased risk of fraud, identity theft, and misuse," Opp. at 16-17, and seek to distinguish *Medoff v. Minka Lighting, LLC*, 2023 WL 4291973, at *9 (C.D. Cal. May 8, 2023) and *Pisciotta v. Old Nat. Bancorp*, 499 F.3d 629, 635 (7th Cir. 2007) by suggesting that they allege "specific instances of actual harm." Opp. at 17 n.3. But Plaintiffs' allegations are indeed similar to those in *Medoff* and *Pisciotta*. In *Medoff*, the plaintiff alleged:

> that his name and social security number were accessed during the breach and that an attorney for Defendant confirmed that his social security number was compromised during the breach . . . that his information was posted on the Dark Web to a forum used by malicious actors. As a result of these events, Plaintiff alleges that he suffered a variety of injuries, including: 1) lost time responding to issues relating to the data breach through monitoring his accounts and credit score; 2) the diminution in the value of his PII; 3) annoyance, interference, anxiety and increased concerns for his loss of privacy; and 4) a substantial risk of fraud, identity theft, and misuse of his PII.

Medoff, 2023 WL 4291973, at *9. The court correctly rejected the allegations as "generalized" and "too speculative to constitute a cognizable injury." *Id.*; *accord Pisciotta*, 499 F.3d at 639 ("Without more than allegations of increased risk of future identity theft, the plaintiffs have not suffered a harm that the law is prepared to remedy."). The same result should occur here.

B. Plaintiffs Fail to State a Claim for Breach of Implied Contractual Duty

Plaintiffs do not state a plausible claim for breach of "implied contract" because "courts have consistently held that the fact that a defendant required plaintiffs to provide personal information does not alone support the inference that the parties agreed for the defendant to

secure this information." Mot. at 18 (collecting cases).

Plaintiffs call the precedent and Prospect's reliance on it "unpersuasive," Opp. at 24, and attempt to save their claims by pointing to "merchant-consumer" cases in which (1) the merchant invited the consumer to use his/her credit and debit cards at its establishments and (2) there were actionable statements made in the merchant's privacy policy. Opp. at 24. By contrast, Plaintiffs themselves nowhere allege that Prospect "invited" Plaintiffs to "use" debit or credit card information at Prospect's "establishment," nor do Plaintiffs point to any policy language on point. Instead, Plaintiffs attempt to proceed in federal court solely on the allegation that "in delivering their Private Information to Defendant and providing paying for healthcare services, Plaintiffs and Class Members intended and understood that Defendant would adequately safeguard the data." Opp. at 26. This is not a basis for claiming an implied contract. Instead, this type of conclusory, self-serving statement is precisely what the Third Circuit forbid in *Longenecker-Wells v. Benecard Servs. Inc.,* 658 F. App'x 659, 663 (3d Cir. 2016) and other Rule 12(b)(6) cases.

C. Plaintiffs Fail to State a Claim of an Invasion of Privacy

There are no facts alleged supporting a claim of invasion of privacy under Pennsylvania common law or under the California constitution, because both Pennsylvania and California law require an intentional intrusion by the defendant, and Plaintiffs conspicuously allege that the cyber hackers (and not Prospect) committed the intentional intrusion. Motion at 19-20.

In response, Plaintiffs abandon all credibility and allege that Prospect "knowingly configured its systems in a way that was vulnerable to foreseeable criminal activity." Opp. at 27. According to Plaintiffs, Prospect intentionally subjected itself to a paralysis of its health system and millions of dollars in losses. This preposterous charge is a nothing but a bare assertion lacking any factual support, because none could credibly exist. *See* Compl. ¶¶ 331, 335. Indeed,

this allegation seeks to bootstrap the mere fact of a ransomware attack by a third party into a claim of intentional invasion of privacy by the victim of that attack, Prospect. That is not what "intentional" means under invasion-of-privacy law. *See O'Donnell v. United States*, 891 F.2d 1079, 1083 (3d Cir. 1989) ("[T]he intrusion, as well as the action, must be intentional."); *In re Am. Med. Collection Agency, Inc. Customer Data Sec. Breach Litig.* ("AMCA II"), No. CV 19-MD-2904, 2023 WL 6216542, at *5 (D.N.J. Sept. 21, 2023) (dismissing privacy claim where unauthorized disclosure occurred because of Defendants' claimed failure "to implement and maintain reasonable safeguards" and was therefore not intentional); *Kirsten v. California Pizza Kitchen, Inc.*, 2022 WL 16894503, at *4 (C.D. Cal. July 29, 2022) (conclusory allegations that the "the Defendant intentionally failed to keep Plaintiffs' PII safe" were not sufficient to withstand a motion to dismiss where "Plaintiffs have not provided anything specific regarding whether or how Defendant knew its security was deficient or any other allegations indicating that Defendant intentionally allowed unauthorized access to Plaintiffs' PII."). The fact that a ransomware hacker was able to intrude into the system, as alleged by Plaintiffs, does not mean that somehow Prospect intended to damage its own health system or make patient information accessible. And indeed, stripped of conclusory assertions, Plaintiffs allege no facts to that effect.

D. Plaintiffs Fail to State a Claim Under the California Medical Information Act (CMIA)

Plaintiffs' CMIA claim lacks necessary factual allegations to proceed past the pleading stage because Plaintiffs do not allege facts that Prospect's purported negligence caused the third party's cyber attack or caused a third party to access and view their medical information. Mot. at 22. Plaintiffs now withdraw their claim under Cal. Civ. Code § 56.10, and only assert claims under § 56.36 and § 56.101(a), CMIA's negligence provisions. As set forth above, because Plaintiffs fail to allege facts showing negligence on the part of Prospect, their CMIA claim also

evaporates. But even if Plaintiffs plausibly allege negligence (and they do not), they must still show that their "medical information" was accessed and there was an "actual breach of confidentiality." *Sutter Health v. Superior Court*, 227 Cal. App. 4th 1546, 1559 (Cal. Ct. App. 2014). They allege no such thing.

Plaintiffs instead rely on their general allegations that, as a result of the data breach, certain diagnosis information, lab results, prescription information, and treatment information was "exfiltrated." Opp. at 31, n. 6 (citing Compl. ¶¶ 67, 68, 230). But those allegations do not show that *their* information was "actually viewed by an unauthorized person." *Sutter Health*, 227 Cal. App. 4th at 1550. *In re Solara Medical Supplies, LLC Customer Data Security Breach Litigation,* which plaintiffs rely upon (Opp. at 32), is instructive. There, the Court found persuasive that they "pled an increase in *medical-related* spam emails and phone calls following the data breach." 613 F. Supp.3d 1284, 1299 (S.D. Cal. 2020) (emphasis added). Here, Plaintiffs allege credit card fraud, written communications regarding tax returns, student loans, and bank accounts, and other *financial-related* harms. *See* Motion at 10 (listing financial-related allegations). Even if those allegations could be connected to the data breach, they do not show that any of Plaintiffs' *medical* information was actually viewed or accessed during the data breach. Plaintiffs' CMIA claims should therefore be dismissed.

E. Plaintiffs Fail to State a Claim Under the California Unfair Competition Law (UCL)

As to Plaintiffs' UCL claim, still fail to show statutory-specific standing. Plaintiffs rely upon their "benefit-of-the-bargain" theory that they "overpaid for Defendant's services" on the understanding that part of those payments would go towards data security. Opp. at 34. But those conclusory allegations—which fail to articulate what services were paid for, when services were paid for, or any "bargain struck" between Prospect and the Plaintiffs (as opposed to their health

insurance provider)—are wholly insufficient. *See Moore v. Centrelake Med. Grp., Inc.*, 83 Cal. App. 5th 515, 527 (Cal. Ct. App. 2022) (finding benefit of bargain theory sufficient when plaintiffs "enter[ed] contracts with Centrelake and accept[ed] its pricing terms."); *Solera*, 613 F.Supp. at 1293 (direct-to-consumer medical provider); *Marriott Int'l, Inc. Customer Data Security Breach Litig.*, 440 F.Supp.3d 447, 492 (D. Md. 2020) (Marriott guests).

Even if they were to be found to somehow have statutory standing, Plaintiffs recognize that their UCL claims are ultimately incompatible with their other claims at relief; they instead argue that the UCL claims should not be dismissed "at this stage." Opp. at 36. But the UCL claims are not "alternative remedies"; they are only viable if no other adequate remedy at law exists. Plaintiffs' pursuit of monetary damages is a concession that there is an adequate remedy at law. Accordingly, the Court should dismiss Plaintiffs' UCL claim. *In re Ambry Genetics Data Breach Litig.*, 567 F. Supp. 3d 1130, 1147 (C.D. Cal. 2021).

CONCLUSION

Prospect respectfully moves that the Court grant its Motion. Prospect requests oral argument on its Motion.

May 23, 2024

Respectfully submitted,

/s/Luke P. McLoughlin
DUANE MORRIS LLP
Alan C. Kessler
Luke P. McLoughlin
Ryan Monahan
Lauren Pugh
30 S. 17th Street
Philadelphia, PA 19103
LPMcLoughlin@duanemorris.com

-and-

Gerald L. Maatman Jr.
Jennifer A. Riley
DUANE MORRIS LLP
190 South LaSalle Street, Suite 3700
Chicago, IL 60603-3433

Counsel for Prospect Medical Holdings, Inc.

CERTIFICATE OF SERVICE

I hereby certify that on May 23, 2024, a true and correct copy of Defendant Prospect Medical Holdings, Inc.'s Reply in Support of Defendant's Motion to Dismiss was electronically filed with the Court, and served upon all counsel of record via the Court's CM/ECF system.

/s/Luke P. McLoughlin
Luke P. McLoughlin